Teemu Wiander

# MISSIOKRIITTINEN ESINEIDEN INTERNET VIRANOMAISTOIMINNASSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2018

# TIIVISTELMÄ

Wiander, Teemu
Missiokriittinen esineiden internet viranomaistoiminnassa
Jyväskylä: Jyväskylän yliopisto, 2018, 25 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Makkonen, Pekka

Esineiden internet on uudenlainen, noususssa oleva, ICT-alan paradigma. Sen nähdään muuttavan merkittävästi eri toimialoja, tehostavan työntekoa ja uudistavan organisaatioita. Yleistymisen myötä myös viranomaisten kiinnostus esineiden internetin hyödyntämiseen on lisääntynyt. Viranomaisille sopivaa missiokriittistä esineiden internetiä ei ole kuitenkaan kovin tarkkaan määritelty toistaiseksi. Lisäksi ison kokonaiskuvan saaminen aiheesta on ollut hankalaa.

Missiokriittinen esineiden internet on kriittisiin käyttöympäristöihin suunnattu esineiden internetin ilmentymä. Missiokriittisyyden tunnistaa siitä, että missiokriittisen järjestelmän vikautuessa vahingot ovat potentiaalisesti merkittäviä, tai se voi johtaa ihmishengen vaarantumiseen.

Tutkielmassa tarkastellaan missiokriittistä esineiden internetiä, sen rakennetta ja huomionarvoisia näkökulmia viranomaisen näkökulmasta. Tutkielmassa esitellään missiokriittisen esineiden internetin teknologiapino. Lisäksi esitellään missiokriittisen esineiden internetin keskeiset haasteet sekä keskustellaan sen hyötyjen saavuttamisesta. Tutkielman tuloksia voidaan hyödyntää käytännössä missiokriittisiä esineiden internet -toteutuksia suunniteltaessa tai niitä hankittaessa.

Asiasanat: Missiokriittinen esineiden internet, IoT, sensoriverkot

# ABSTRACT

Wiander, Teemu
Mission Critical Internet of Things in Public Safety and Disaster Relief
Jyväskylä: University of Jyväskylä, 2018, 25 pp.
Information Systems, Bachelor's Thesis
Supervisor: Makkonen, Pekka

The Internet of Things (IoT) is a new, emerging paradigm in the ICT industry. It is seen to significantly transform various industries, streamline work and to expand organizational boundaries. As IoT has become increasingly common, authorities' interest to achieve benefits and efficiencies from IoT has also emerged. However, mission critical IoT (MC-IoT) fit for public safety and disaster relief use has not been defined very clearly. In addition, getting a big picture of MC-IoT has been difficult.

MC-IoT is a manifestation of IoT to fit critical use context. Mission critical systems are characterized by when it fails, the damage is potentially significant, or it can endanger human life.

This thesis examines MC-IoT, its structure and notable perspectives from public safety and disaster relief point of view. The thesis introduces a technology stack for mission critical internet of things. It will also include key challenges of the MC-IoT as well as discuss how to achieve desired benefits from it. The results of the thesis can be used in practice when designing MC-IoT solutions or when preparing to acquire one.

Keywords: Mission Critical Internet of Things, IoT, sensor networks

## KUVIOT

KUVIO 1 Esineiden internetin teknologiapino ..... 10
KUVIO 2 Missiokriittisen esineiden internetin teknologiapino ..... 13

## TAULUKOT

TAULUKKO 1 Missiokriittisen esineiden internetin haasteita..... 18

# SISÄLLYS

TIIVISTELMÄ
ABSTRACT
KUVIOT
TAULUKOT
SISÄLLYS

1 JOHDANTO ... 6

2 ESINEIDEN INTERNET ... 8
2.1 Esineiden internetin rakenne ... 9
2.2 Esineiden internet ja arvon muodostuminen ... 10

3 MISSIOKRIITTINEN ESINEIDEN INTERNET ... 12
3.1 Missiokriittisen esineiden internetin teknologiapino ... 13
3.1.1 Esineet ja käyttölaitteet ... 13
3.1.2 Yhteyskeinot ... 14
3.1.3 Sovellukset ... 14
3.1.4 Integraatio organisaation järjestelmien kanssa ... 15
3.1.5 Ulkoiset informaatiolähteet ... 15
3.1.6 Kyberturvallisuus ... 15
3.1.7 Turvallisuus ... 16
3.1.8 Luotettavuus ... 16
3.1.9 Reaaliaikaisuus ... 16
3.2 Missiokriittisen esineiden internetin haasteet ... 17

4 YHTEENVETO ... 20

LÄHTEET ... 22

# 1 JOHDANTO

General Electricin (GE) liikevaihto koostui yli vuosisadan ajan lähinnä teollisen laitteiston myymisestä sekä korjauspalveluista. 2010 luvulle tultaessa uudenlaiset kilpailijat, kuten teknologiayritykset IBM ja SAP sekä Big Dataa hyödyntävät startupit alkoivat uhata GE:n markkina-asemaa. Näiden yritysten liiketoimintamalli oli fundamentaalisesti erilainen: Luotettavien laitteiden hankkimisen sijaan asiakas sai hyötyä laitteiden sensoreista kerättyyn dataan perustuvasta analytiikasta ja sen hyödyntämisestä toiminnan tehostamiseksi. Muuttuneeseen markkinatilanteeseen reagoidakseen, GE käynnisti miljardiluokan esineiden internetiin pohjaavan hankkeen, jonka nimeksi muodostui teollinen internet.

Teollisen internetin myötä GE alkoi asentaa tuotteisiinsa digitaalisia sensoreita, jotka kommunikoivat pilvialustan kanssa. Pilvialusta mahdollisti edistyneen analytiikan sekä muiden ohjelmisto-ominaisuuksien hyödyntämisen asiakkaan liiketoiminnan tehostamiseksi. Käytännön muutos tapahtui siinä, että GE kykeni myymään esimerkiksi lentokoneen turbiinin sijaan liiketoiminnan hyötyjä, kuten enemmän lentomaileja vuodessa tai vähentynyttä seisonta-aikaa. (Iansiti ja Lakhani, 2014).

Esineiden internet (Engl. Internet of Things), johon myös edellä mainittu teollinen internet kuuluu, on saanut viime vuosina runsaasti huomiota teollisuudenalalta, tieteentekijöiltä sekä julkishallinnoilta. Ilmiölle löytyy myös selitys, sillä Big Datan ja esineiden internetin viimeaikaiset edistysaskeleet tuovat mukanaan ennennäkemättömiä mahdollisuuksia datakeskeiseen toimintaan ja päätöksentekoon (Belanger ja Xu, 2015). Esineiden internetin hyödyntäminen lisääntyykin kovaa vauhtia. Vuonna 2020 maailmassa tulee olemaan arviolta 20,8 miljardia internetiin kytkettyä laitetta (Gartner, 2018). Pelkästään teollisen internetin laitteita tulee olemaan vuoteen 2020 mennessä kolminkertainen määrä verrattuna vuoteen 2017 (Gartner, 2017).

OECD:n (2012) arvion mukaan valtiot tulevat olemaan keskeisessä asemassa esineiden internetin käyttöönotossa ja sen hyödyntämisessä. Esineiden internet onkin nyt tekemässä tuloaan myös viranomaisten, kuten poliisin tai palokunnan, käyttöön. Tämä näkyy myös esimerkiksi vuoden 2018 Critical Communications World -messuilla, jossa tulee olemaan esillä ratkaisuja esinei-

den internetin hyödyntämisessä kriittisen kommunikaation apuna (Critical Communications World, 2018). Viranomaisilla on kuitenkin erityisiä tarpeita esineiden internetin suhteen, ja tässä yhteydessä usein puhutaankin missiokriittisestä esineiden internetistä. Missiokriittiselle esineiden internetille ei kuitenkaan ole toistaiseksi selkeää määritelmää, eikä varsinkaan viranomaisten näkökulmasta. Tämän tutkielman tarkoitus on selvittää, mistä missiokriittisessä esineiden internetissä on kyse.

Tämän tutkielman tutkimuskysymykset ovat:

- Mistä missiokriittinen esineiden internet koostuu?
- Millaisia näkökulmia on otettava huomioon missiokriittisen esineiden internetin toteutuksessa?

Näitä kysymyksiä tarkastellaan missiokriittisen esineiden internetin asiakasorganisaation näkökulmasta. Tutkielman tavoite on siis tuoda esille missiokriittisen esineiden internetin hankinnan tueksi tai siihen pohjautuvien digitalisoitujen palveluiden suunnitteluun tarvittavaa ymmärrystä.

Tutkielma on toteutettu kirjallisuuskatsauksena, ja sen lähdemateriaali on kerätty hyödyntäen Google Scholar -palvelua. Kaikki lähdemateriaali on ollut englanninkielistä. Lähteissä on pyritty painottamaan korkeatasoisissa vertaisarvioiduissa akateemisissa julkaisuissa julkaistuja artikkeleita siten, että korkeampiarvoisen julkaisun artikkelit saavat enemmän painoa aina, kun mahdollista. Julkaisujen arvon määrittelyssä on hyödynnetty Julkaisufoorumin Julkaisukanavahakua. Akateemisten, vertaisarvioitujen, artikkeleiden lisäksi tietoa on kerätty hakien Googlella, sekä arvostetuilta alan tahoilta, kuten Harvard Business Review ja IEEE.

Tutkielma etenee tästä eteenpäin seuraavalla tavalla. Toisessa luvussa pyritään muodostamaan käsitys esineiden internetistä. Lisäksi siinä pohditaan esineiden internetin roolia arvonmuodostuksen osatekijänä.

Kolmannessa luvussa määritellään missiokriittinen esineiden internet viranomaisnäkökulmasta ja esitellään sen rakenne. Luvussa esitellään missiokriittisen esineiden internetin teknologiapino, sekä pohditaan missiokriittisen esineiden internetin haasteita viranomaisorganisaatioille.

Neljännessä luvussa on yhteenveto sekä pohdintaa. Lisäksi siinä nostetaan esille tutkimusprosessissa esiintyneitä haasteita, sekä pohditaan jatkotutkimusaiheita.

# 2 ESINEIDEN INTERNET

Esineiden internet on uudenlainen ICT-alan paradigma. Toistaiseksi sille ei ole muodostunut yhtä selkeää määritelmää (IEEE Internet Initiative, 2015, Atzori ym., 2010). Määritelmän muodostamiseksi, sekä esineiden internetin standardoimiseksi on kuitenkin muodostettu useita toimielimiä (IEEE Internet Initiative, 2015, Agarwal ja Dey, 2016, AIOTI, 2015, Open Connectivity Foundation, 2018).

IEEE:n (2014) kuvauksen mukaan esineiden internet on ”verkko esineistä, joihin kuhunkin on upotettu sensoreita, ja jotka on yhdistetty internetiin”. Tämä määritelmä saattaa kuitenkin olla liian rajoittunut, sillä esineiden internetin mahdollistavista tiedonsiirtoprotokollista harva kuljettaa tietoa internetin välityksellä (Al-Fuqaha ym., 2015). Laajempi määritelmä olisi, että esineiden internet mahdollistaa ”esineiden”, kuten RFID tagien, sensoreiden, käyttölaitteiden, matkapuhelinten, ym. välisen interaktion sekä yhteistyön saavuttaakseen yhteisiä päämääriä (Giusto ym., 2010). Atzori ja muut määrittelevät, että esineiden internet on standardeja (esim. HTTP) hyödyntävä verkko älykkäitä esineitä, joihin voi viitata yksilöllisesti.

Esineiden internetille on useita eri käyttökohteita, kuten liikennevälineet, älykaupungit, terveydenhuolto, turvallisuusala ja useita muita (Sundmaeker ym., 2010, Atzori ym., 2010). Esineiden internetiä voidaankin tarkastella alustana (Wortmann ja Flüchter, 2015) uusille digitaalisille palveluille, jotka kykenevät ympäristöstä kerätyn datan analysoinnin perusteella automaattiseen päätöksentekoon sekä toimimaan päätösten mukaisesti (Beverungen ym., 2017, Al-Fuqaha ym., 2015).

Beverungen ja muut (2017) ovat koostaneet esineiden internetin muodostavista esineistä (”älykäs tuote”) kahdeksan tyypillistä ominaisuutta. Kaikkia kahdeksaa ominaisuutta ei esineessä tarvitse esiintyä samanaikaisesti. Nämä kahdeksan ominaisuutta ovat:

1. **Uniikki** - kukin esine on yksilöllisesti tunnistettavissa
2. **Paikkatietoinen** - kukin esine tietää oman sijaintinsa, ja niiden sijaintia voi seurata

3. **Yhdistettävä** - esineet ovat yhdistettävissä muihin resursseihin hyödyntäen standardoituja yhteysprotokollia
4. **Sensorit** - esineet kykenevät keräämään ympäristöstään dataa (esim. valon määrä, lämpötila, kosteus)
5. **Tiedon tallennus ja -käsittely** - kullakin esineellä on sisäinen muisti sekä prosessori paikallista tiedonkäsittelyä varten
6. **Aktuaattori** - esineet kykenevät manipuloimaan fyysistä ulottuvuutta (esim. kytkin, venttiili)
7. **Rajapinta** - esineet kykenevät paikallisiin interaktioihin toisten esineiden tai ihmisten kanssa
8. **Näkymätön** - esineet kykenevät autonomiseen toimintaan, eivätkä välttämättä vaadi lainkaan käyttäjän huomiota

Esineiden internet on siis ainakin joukko älykkäitä esineitä, jotka kykenevät aistimaan ja manipuloimaan ympäristöä, ja jotka kykenevät kommunikoimaan keskenään, ja jotka kykenevät toimimaan autonomisesti.

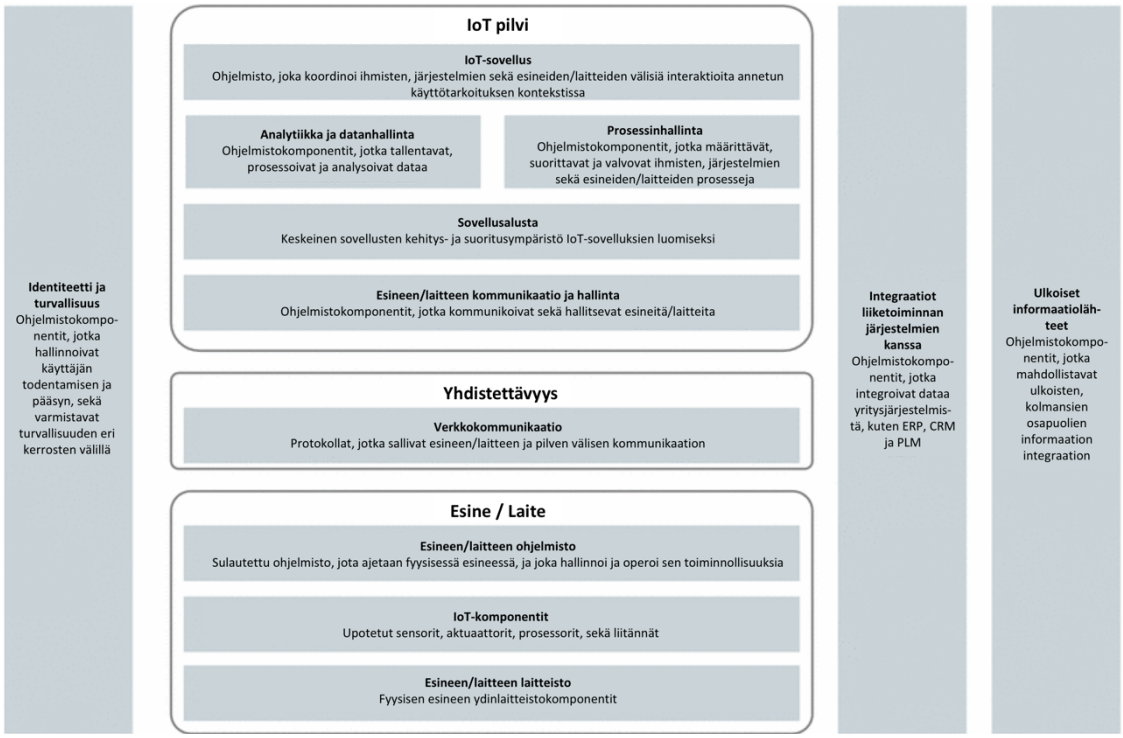
Seuraavissa aliluvuissa pyritään muodostamaan käsitys esineiden internetin rakenteesta, ja pohtimaan sen roolia arvonkehityksessä.

## 2.1 Esineiden internetin rakenne

Atzori ja muut (2010) ovat esittäneet esineiden internetin kiteytyvän kolmeen näkökulmaan. Ensimmäinen on ”esine”-painotteinen näkökulma, jolla viitataan sensoreilla varustettuihin esineisiin, joilla voi olla myös älyominaisuuksia, ja voivat olla kykeneviä autonomiseen toimintaan. Toinen näistä painottuu ”internet”-käsitteeseen, joka viittaa esineiden internetin rooliin esineiden välisten interaktioiden välittäjänä ja rajapintana. Kolmas on esineiden internetin semantiikkaan painottunut näkökulma, jolla pyritään ymmärtämään, kuinka esineiden internetin keräämää tietoa käytetään, esitetään ja tallennetaan. Kirjoittajat esittävät, että esineiden internetin paradigma on näiden kolmen näkökulman yhdistelmä.

Porter ja Heppelmann (2014) ovat tunnistaneet samat kolme näkökulmaa, kuin Atzori ja muut (2010), käsitellessään nk. älykkäitä tuotteita, jotka ovat yksiä esineiden internetin käytännön sovelluksista. He ovat rakentaneet näiden kolmen näkökulman ympärille mallinnuksen älykkäiden tuotteiden teknologiapinosta. Heidän mallinsa esittelee kolme lisäelementtiä, jotka liittyvät osana älykkäiden tuotteiden ekosysteemiin: ulkoiset informaatiolähteet, integraatiot yritysjärjestelmien kanssa, sekä identiteetin hallinta ja turvallisuus.

Wortmann ja Flüchter (2015) ovat tehneet tähän malliin perustuen esineiden internetille vastaavan mallin kuvaamaan esineiden internetin teknologiapinoa (kuvio 1). Mallissa on kolme pääelementtiä, jotka ovat esine/laite, yhdistettävyys tavat sekä esineiden internetin pilvi (”IoT pilvi”). Malli siis sisältää samat kolme näkökulmaa, kuin Atzori ja muut (2010) ovat kuvanneet, mutta mallissa on menty käytännönläheisemmälle tasolle. Mallista löytyy myös samat kolme lisäelementtiä, kuin Porter ja Heppelmann (2014) ovat esittäneet.




KUVIO 1 Esineiden internetin teknologiapino (Wortmann ja Flüchter, 2015)

## 2.2 Esineiden internet ja arvon muodostuminen

Kuten jo edellä käsiteltiin, esineiden internetiä käsitellään usein teknologialähtöisesti. On kuitenkin otettava huomioon, että esineiden internetillä pyritään viimekädessä ratkaisemaan organisaatioiden haasteita tai tuottamaan muita hyötyjä, kuten esimerkiksi johdannossa mainittu GE:n tapaus osoittaa. Kirjallisuudessa esimerkiksi Vargo ja Lusch (2004) ovat edistäneet näkökulmaa, jossa tuotteeseen, kuten tässä tapauksessa esineiden internetiin, ei voida tuottaa arvoa sisäänrakennettuna, vaan arvo syntyy asiakkaan käyttäessä sitä. Esineiden internetin hyötyjen saavuttamiseksi tarkastelemme siis esineiden internetiä yhtenä resurssina arvon tuotannossa. Seuraavaksi nostetaan esille näkökulma esineiden internetin, digitaalisten palveluiden sekä arvon yhteiskehityksen yhteydestä.

2000-luvulla olemme nähneet siirtymisen tuotelähtöisestä markkinoinnin ajattelutavasta palvelulähtöiseen ajattelutapaan, jossa korostuu asiakkaan rooli arvontuottajana (Vargo ja Lusch, 2004, Vargo ja Lusch, 2007, Grönroos ja Voima, 2013). Tämän kehityksen myötä myös arvontuotantoa on alettu tarkastella arvontuotantoverkkona, jossa useat toimijat toimivat yhdessä arvon tuottamiseksi. Informaatioteknologiaa mahdollistaa resurssien ja tietämyksen integroinnin ja jakamisen arvontuotantoverkossa (Lusch ja Nambisan, 2015).

Vargo ja Lusch (2004) määrittelevät palvelun ”tiedon ja taidon soveltamisena läpi toimenpiteiden, prosessien ja suoritusten, hyödyttääkseen toista entiteettiä tai entiteettiä itseään”. Näkemyksen mukaan palvelun tuotantoon kuuluu aina vähintään kaksi osapuolta (palveluntuottaja ja asiakas), jotka molemmat osallistuvat omalla panoksellaan palvelun tuotantoon. Tällöin voidaan puhua arvon yhteistuotannosta (Vargo ja Lusch, 2004, Grönroos ja Voima, 2013). Lusch ja Nambisan (2015) ovat kuvanneet palvelulle kolme keskeistä teemaa. Nämä ovat palveluekosysteemi, palvelualusta sekä arvon yhteiskehitys.

Palveluekosysteemillä tarkoitetaan ”suhteellisen itsenäistä, itsesäätyvää rakennelmaa, joka koostuu enimmäkseen löyhästi yhdistellyistä resursseja integroivista toimijoista”. Näin ollen esineiden internetiä voidaan tarkastella palveluekosysteeminä, jossa älykkäät sensoreilla varustetut esineet ovat edellä mainittuja ”resursseja integroivia toimijoita” (Beverungen ym., 2017). Toisaalta esineiden internetin vahvuus on siinä, että se yhdistää samaan palveluekosysteemiin esineiden lisäksi myös kumppanit ja asiakkaat (Kranz, 2017).

Palvelualustalla tarkoitetaan modulaarista rakennelmaa, joka fasilitoi toimijoiden ja resurssien välisiä interaktioita palveluekosysteemissä. Palvelualustan modulaarisuus johtaa siihen, että palvelualustan komponentteja voidaan kierrättää ja varioida asiakkaan tarpeiden mukaisesti (Tuunanen ja Cassab, 2011). Esineiden tai laitteiden, ohjelmistojen, organisaation kykyjen sekä liiketoimintojen modularisointi yleistyy koko ajan. Moduulien ovat sitä hyödyllisempiä, mitä useampaan eri käyttötapaukseen ne sopivat hyödynnettäväksi (Pagani, 2013). Wortmannin ja Flüchterin (2015) esineiden internetin teknologiapinossa palvelualustalla viitataan pilvialustaan (”IoT cloud”), joka mahdollistaa esineiden, ihmisten sekä tietojärjestelmien väliset vuorovaikutukset. Pilvialustan moduuleita (esim. tiedonlouhintasovellus tai käyttöliittymä) voidaan korvata tai kierrättää eri asiakkaitten, kuten poliisi tai pelastuslaitos, tarpeisiin.

Arvon yhteiskehitystä ovat ne prosessit ja aktiviteetit, jotka luovat pohjan resurssien integroinnille sekä liittävät eri toimijarooleja palveluekosysteemiin. Palvelulähtöisessä ajattelutavassa arvoa ei voida pakata tuotteeseen, tai tässä tapauksessa esineeseen, tehtaalla, vaan se syntyy käytettäessä (Vargo ja Lusch, 2004). Tästä johtuen esineiden internetin käyttöönotossa tulisi ottaa ensisijaisesti huomioon ratkaistava liiketoiminnallinen haaste, ja prosessit, joiden avulla esineiden internetin ratkaisun arvolupaus saadaan toteutumaan (Kranz, 2017).

Tässä tutkielmassa ei tutkita syvällisemmin esineiden internetiä digitalisoitujen palveluiden näkökulmasta. Esineiden internetin hankintaa ja vaatimuksia suunniteltaessa on kuitenkin merkittävää hyötyä ymmärtää esineiden internet arvon muodostumisen kontekstissa, sillä loppukäyttäjälle tuote toimitetaan aina palvelun muodossa, kuten edellä argumentoitiin.

# 3 MISSIOKRIITTINEN ESINEIDEN INTERNET

Viranomaisten ICT järjestelmien, ja etenkin kommunikaatiojärjestelmien, yhteydessä käytetään usein termiä ”missiokriittinen”. Järjestelmä on missiokriittinen eli turvallisuuskriittinen, kun sen vika tai kaatuminen voi johtaa vakaviin seurauksiin, kuten merkittäviin vahinkoihin tai ihmishengen vaarantumiseen. Itse asiassa mikä tahansa järjestelmä, jonka pettäminen ei ole hyväksyttävää, voidaan tulkita missiokriittiseksi (Knight, 2002).

Esimerkiksi yleisen turvallisuuden viranomaisten (esim. poliisi, rajavartiolaitos) järjestelmät luetaan missiokriittisiksi (Fraga-Lamas ym., 2016). Järjestelmiä käytetään usein haastavissa ja nopeasti muuttuvissa käyttöympäristöissä sekä niiden toiminnan varaan pitää kyetä luottamaan hengellään. Tästä syystä on erittäin tärkeää, että tieto kulkee perille luotettavasti ja ajoissa. Jotta viranomaiset voisivat luottaa esineiden internetiin työssään, tulee selvittää, pitäisikö tiettyjä esineiden internetiin pohjautuvia ratkaisuja kohdella missiokriittisinä.

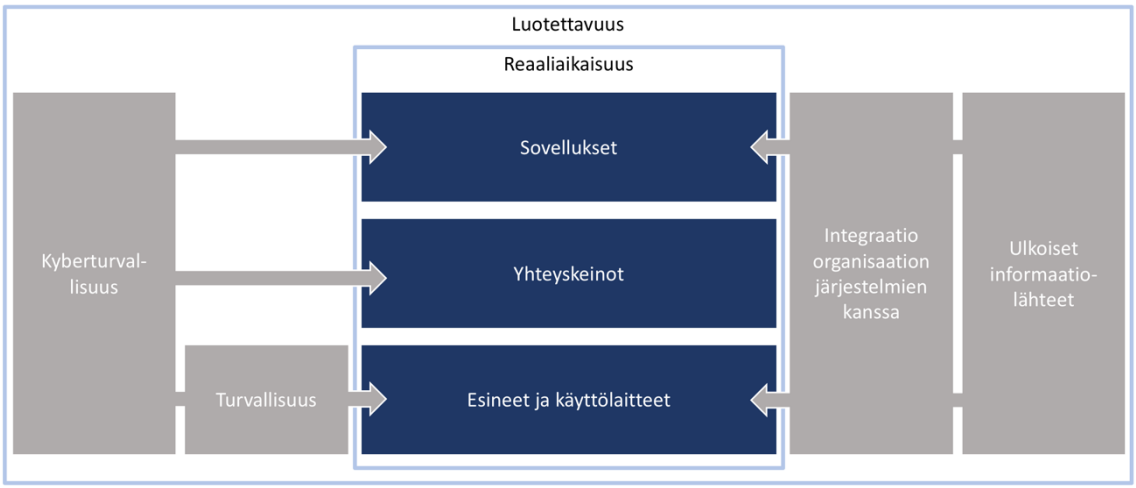
Missiokriittinen esineiden internet rakentuu esineiden internetin pohjalle. Voidaan siis katsoa sen perivän esineiden internetin rakenteen, kuten edellisessä luvussa kuvattiin. Missiokriittiselle esineiden internetille kuuluu kuitenkin tiettyjä ominaispiirteitä, joiden perusteella se eroaa esineiden internetistä. Nämä piirteet ovat tyypillisesti lisävaatimuksia. Ciccozzi ja muut (2017) ovat havainneet missiokriittiselle esineiden internetille neljä tyypillistä ominaispiirrettä:

1. **Luotettavuus** - missiokriittisen esineiden internetin tulee olla äärimmäisen luotettava, vikasietokykyinen, sekä sillä pitää olla korkea saatavuus
2. **Turvallisuus** - missiokriittinen esineiden internet kykenee tunnistamaan ja ehkäisemään esineiden epätarkoituksenmukaista käytöstä
3. **Kyberturvallisuus** - kyberturvallisuus koostuu identiteetin ja pääsynhallinnasta sekä kyberturvallisuuslainsäädännön ja regulaation noudattamisesta
4. **Reaaliaikaisuus** - missiokriittisen järjestelmän on kyettävä datan reaaliaikaiseen keräämiseen, manipuloimiseen, löytämiseen sekä visualisointiin

Tässä luvussa pureudumme esineiden internetiin missiokriittisessä kontekstissa. Luvussa esitellään missiokriittisen esineiden internetin teknologiapino sekä esitellään sen keskeisiä haasteita.

## 3.1 Missiokriittisen esineiden internetin teknologiapino

Koska missiokriittisellä esineiden internetillä on edellä mainittuja erityispiirteitä, ehdotan Wortmannin ja Flüchterin (2015) esineiden internetin teknologiapinoon (kuvio 1) perustuvaa uutta, missiokriittiseen ympäristöön soveltuvaa mallia: Missiokriittisen esineiden internetin teknologiapino (kuvio 2). Mallissa sovelletaan esineiden internetin teknologiapinoa niiltä osin, kuin on mahdollista. Malli kuitenkin esittelee kolme uutta elementtiä, eli turvallisuus, reaaliaikaisuus ja luotettavuus. Siinä on myös täsmennetty termistöä missiokriittiseen ympäristöön sopivammaksi. Seuraavaksi tutustumme lähemmin mallin yhdeksään elementtiin.




KUVIO 2 Missiokriittisen esineiden internetin teknologiapino

### 3.1.1 Esineet ja käyttölaitteet

Esineet keräävät kaikenlaista informaatiota ympäristöstä sekä mahdollistavat ympäröivään todellisuuteen vaikuttamisen (Suo ym., 2012). Käyttölaitteet mahdollistavat ihmisen ja esineiden internetin välisen interaktion.

Esineiden internetissä, siispä myös missiokriittisessä esineiden internetissä, laitteet voidaan jakaa kolmeen kategoriaan. Ensimmäinen näistä on yksinkertaiset yhdistetyt sensorit tai aktuaattorit. Näissä ei ole varsinaista logiikka sisäänrakennettuna, vaan ne välittävät dataa tai suorittavat käskyjen mukaisia toimenpiteitä (esim. oven avaus). Toinen kategoria on älykkäät esineet, joiden kahdeksaa tyypillistä ominaisuutta (Beverungen ym., 2017) käsittelimme edelli-

sessä luvussa. Kolmas kategoria on käyttölaitteet, jotka mahdollistavat ihmisen ja esineiden internetin välisen interaktion.

Esineiden internetissä nämä kolme kategoriaa ovat löyhiä. Esimerkiksi älypuhelin mielletään usein käyttölaitteena, mutta siihen upotetut sensorit (kamera, GPS, gyroskooppi, ym.) tekevät siitä myös älykkään esineen.

Missiokriittisessä esineiden internetissä esineiden vaatimuksena voi olla, että niiden tulee toimia äärimmäisissä olosuhteissa (Fraga-Lamas ym., 2016). Huomioon otettavia seikkoja voi olla esimerkiksi esineen IP-luokitus tai lujuus. Olemme silti hiljattain alkaneet tunnistaa valtavirran ja missiokriittisten markkinoiden yhdentymistä. Muutoksen ajuriksi on tutkittu olevan molempien markkinoiden lisääntynyt tarve missiokriittisille ominaisuuksille, kuten luotettavuus tai suorituskyky (Girbal ym., 2013). COTS, eli kaupallisesti ”suoraan hyllyltä” ostettavien (engl. commercial off-the-shelf) laitteiden hyödyntäminen niiden edullisuuden ja saatavuuden vuoksi onkin houkuttelevaa myös missiokriittisissä ratkaisuissa (Fraga-Lamas ym., 2016).

### 3.1.2 Yhteyskeinot

Yhteyskeinot mahdollistavat esineiden ja käyttölaitteiden kommunikoinnin sovelluskerroksen ja toistensa kanssa. Älykkäiden tuotteiden tapauksessa yhteys muodostetaan tyypillisesti esineiden ja pilvipalvelun välille (Wortmann ja Flüchter, 2015, Beverungen ym., 2017). Missiokriittisessä esineiden internetissä, kuten esineiden internetissä yleisestikin, laitteet voivat kommunikoida myös keskenään (Fraga-Lamas ym., 2016, Giusto ym., 2010).

Yhteyskeinoja on monia, ja ne voivat olla sekä langallisia ja langattomia (Al-Fuqaha ym., 2015). Missiokriittisissä toteutuksissa kommunikaatiojärjestelmän täytyy olla vakaa, luotettava, kestävä (Favraud ym., 2016, Fantacci ym., 2016). Tästä syystä missiokriittiset organisaatiot, ja etenkin viranomaiset, käyttävät usein jotain missiokriittiseen kommunikaatioon suunniteltua digitaalista radioteknologiaa, kuten TETRA, TETRAPOL tai P25, kriittiseen kommunikaatioon (Fantacci ym., 2016). Nämä teknologiat sopivat myös käytettäväksi esineiden internetin yhteyskeinona, kuten esimerkiksi Lloret ja muut (2016) ovat maininneet.

Kuten esineiden ja käyttölaitteiden kohdalla, myös yhteyskeinojen kohdalla missiokriittisten organisaatioiden mielenkiinto kaupallisten verkkojen hyödyntämiseen on noussut viime vuosina. Toistaiseksi kaupallisissa LTE-verkoissa on kuitenkin haasteena huoli palvelun tasosta ja turvallisuudesta (Fantacci ym., 2016). LTE-standardin kehityksestä vastaava 3GPP onkin reagoinut tähän muutokseen, ja missiokriittisen kommunikaation edellyttämien ominaisuuksien standardointi osaksi LTE standardia on alkanut (3GPP, 2017).

### 3.1.3 Sovellukset

Sovelluskerkkoksessa ratkaistaan esineiden internetin semantiikkaan liittyviä haasteita, eli kuinka tietoa tallennetaan, hyödynnetään ja esitetään (Atzori ym., 2010). Wortmannin ja Flüchterin (2015) esittämä pilvikerros ei ole sopiva ku-

vaamaan missiokriittistä järjestelmää, sillä sovellukset voivat sijaita yksityisessä pilvessä, julkisessa pilvessä tai täysin erillään pilvestä (Fraga-Lamas ym., 2016). Myös Fraga-Lamas ja muut (2016) ovat päätyneet samanlaiseen kolmikerroksiseen malliin, mitä tässä tutkielmassa esitetyn missiokriittisen esineiden internetin mallin pääelementit ovat.

Sovelluskerrokseen voidaan sijoittaa useita erityyppisiä sovelluksia, kuten kommunikaatio- ja laitehallintasovelluksia, sovellusalustoja, analytiikka- ja datanhallintasovelluksia, ja prosessinhallintasovelluksia (Wortmann ja Flüchter, 2015). Datan hyödyntämisestä ja analytiikasta saadaan merkittäviä hyötyjä missiokriittisen toiminnan tukemiseksi ja tehostamiseksi (Chen ym., 2012). Yksi näistä hyödyistä on koneavusteinen strateginen päätöksenteko (Newell ja Marabelli, 2015). Siispä sovellusvalintoihin tulisi kiinnittää erityistä huomiota missiokriittisen esineiden internetin hyötyjen saavuttamiseksi.

Kuten aiemmin jo mainittiin, missiokriittisen esineiden internetin tulee olla reaaliaikainen, ja sillä täytyy olla korkea saatavuus (Ciccozzi ym., 2017). Haasteeksi voi kehkeytyä yksittäisen kohdan vikaantuminen järjestelmässä. Yksi ratkaisu tähän saatavuusongelmaan voi olla fog computing, jossa paikallisverkko ottaa hoitaakseen pilvipalvelun tehtäviä, eli IaaS, PaaS ja SaaS toimintoja (Bonomi ym., 2012, Fraga-Lamas ym., 2016). Fog computing hajauttaa resurssit useiden esineiden internetiin kytkettyjen laitteiden välillä ja luo niistä virtuaalisen alustan, jolla sovelluksia voidaan ajaa paikallisesti itsenäisesti tai pilven rinnalla (Chiang ja Zhang, 2016). Missiokriittisessä esineiden internetissä fog computing on yksi mahdollisuus lisätä sovellustasolla esineiden internetin luotettavuutta ja saatavuutta, vaikka tilanteissa, joissa yhteydet voivat olla epävarmat.

### 3.1.4 Integraatio organisaation järjestelmien kanssa

Integraatio organisaation järjestelmien kanssa kattaa ne ohjelmistokomponentit, jotka yhdistävät esineiden internetin esineet ja käyttölaitteet, sekä sovellukset muihin organisaation järjestelmiin, kuten ERP (Wortmann ja Flüchter, 2015).

### 3.1.5 Ulkoiset informaatiolähteet

Esineiden internetin esineitä ja käyttölaitteita, sekä sovelluksia voidaan kytkeä ulkoisiin informaatiojärjestelmiin. Ulkoisia informaatiolähteitä voivat olla esimerkiksi avoimet julkiset informaatiolähteet tai muut kolmannen osapuolen informaatiolähteet (Wortmann ja Flüchter, 2015).

### 3.1.6 Kyberturvallisuus

Missiokriittisen esineiden internetin turvallisuus voidaan jakaa kahteen osaan, joista ensimmäinen on kyberturvallisuus ja toinen on turvallisuus (Ciccozzi ym., 2017). Tämä täsmentää Wortmannin ja Flüchterin (2015) mallia erottamalla nämä elementit omiksi kokonaisuuksikseen.

Yksinkertaisesti asetettuna kyberturvallisuudella pyritään varmistumaan, että ainoastaan sallituilla (engl. authorized) entiteeteillä, eli ihmisillä, laitteilla tai ohjelmistoilla, on pääsy kyseiseen esineiden internetiin (Agarwal ja Dey, 2016). Kyberturvallisuuteen liittyy siis ne ohjelmistokomponentit, jotka varmistavat turvallisuuden esineiden internetin eri kerroksilla, ja vastaavat pääsynhallinnasta (Wortmann ja Flüchter, 2015). Suojauksen tulee kattaa myös fyysiset hyökkäykset, yksityisyyden sekä järjestelmätason luottamuksen (Ciccozzi ym., 2017). Kyberturvallisuutta suunnitellessa on hyvä ottaa huomioon myös regulaatio ja lainsäädäntö (Suo ym., 2012).

### 3.1.7 Turvallisuus

Turvallisuudessa on ennen kaikkea kyse pyrkimyksestä ehkäistä käyttölaitteiden ja esineiden, etenkin aktuaattoreiden, epätarkoituksenmukaista käytöstä (Ciccozzi ym., 2017). Chen ja Helal (2011) ovat sanoneet, että laitteet ovat esineiden internetin päähuolenaihe turvallisuusnäkökulmasta.

Esimerkiksi laitteiden ja sovellusalustojen tulee tietyissä tapauksissa kyetä käsittelemään vanhaa ja uutta koodia samanaikaisesti. Tällöin tarvitaan näiden prosessien tiukka eriyttäminen turvallisuuden takaamiseksi (Fraga-Lamas ym., 2016). Esineet voivat olla virheellisesti ohjelmoitu tai ne voivat häiritä toisia esineitä, jolloin ne voivat vikaantua tai saada muita esineitä vikaantumaan (Chen ja Helal, 2011).

Chen ja Helal (2011) ovat listanneet tekijöitä, jotka vaikuttavat laitteiden turvallisuuteen. Näitä tekijöitä ovat mm. haasteellinen ympäristö, erilaiset häiriönaiheuttajat, väärinkäyttö sekä ohjelmiston tai laitteiston virhetilat.

### 3.1.8 Luotettavuus

Luotettavuus ja reaaliaikaisuus ovat missiokriittisen esineiden internetin teknologiapinossa suoraan teknologian tai ohjelmiston suunnitteluun vaikuttavia vaatimuksia. Tästä syystä ne on lisätty myös tähän malliin.

Missiokriittisessä esineiden internetissä tavoitellaan ultravarmoja ja äärimmäisen saatavuuden (engl. availability) tavoittavia järjestelmiä, joten luotettavuusvaatimus kattaa kaikki sen elementit.

Luotettavuudessa yhdistyy ne tekijät, jotka vaikuttavat käyttäjän luottamukseen järjestelmää kohtaan (Ciccozzi ym., 2017). Macedo ja Silva (2014) ovat jakaneet nämä tekijät kahteen ryhmään: toimintavarmuus (engl. reliability) ja saatavuus. He ovat ehdottaneet redundanssin lisäämistä esineiden internetin kriittisiin osiin varmistaakseen toimintavarmuuden ja saatavuuden.

### 3.1.9 Reaaliaikaisuus

Missiokriittiseltä esineiden internetiltä odotetaan virheettömyyttä sekä ajantasaisuutta. Tämän alueen tutkimustieto keskittyy laajasti reaaliaikaiseen datan keräämiseen, manipulointiin, löytämiseen ja visualisointiin (Ciccozzi ym., 2017).

Reaaliaikaisuus on olennaista ja odotettavaa edistyneen tilannetiedostamisen muodostamiseen päätöksenteon pohjana (Fraga-Lamas ym., 2016). Reaaliaikaisuuteen pyrkimyksestä onkin muodostunut haaste, johon esimerkiksi fog computing tai paikalliset ”minipilvet” voisivat olla ratkaisuja (Bonomi ym., 2012, Fraga-Lamas ym., 2016). Samansuuntaista ajatusta ovat tukeneet myös Atzori ja muut (2010), sillä he ovat esittäneet ratkaisuksi palvelukeskeistä arkkitehtuuria (SOA).

## 3.2 Missiokriittisen esineiden internetin haasteet

Missiokriittiseen esineiden internetiin liittyy edelleen useita eri haasteita. Seuraavaksi kuvataan lähdekirjallisuuden pohjalta keskeisimmiksi nostettuja haasteita. Muutamia näistä ovat ainakin standardoinnin puutteellisuus, skaalautuvuus, yhteentoimivuus sekä turvallisuus ja kyberturvallisuus (Fraga-Lamas ym., 2016). Taulukko 1:ssä on koostettu kirjallisuuden esiin nostamia haasteita missiokriittiseen esineiden internetiin liittyen.

Standardointi on tärkeää, sillä esineiden internetin laitteet ja ohjelmistot ovat heterogeenisiä, mutta niiden oletetaan kykenevän saumattomaan yhteistyöhön. Haaste onkin sen verran merkittävä, että Lee ja Lee (2015) ovat kutsuneet tätä valtavaa eri teknologioiden yhteen saattamista kaaoshaasteeksi. Missiokriittisten järjestelmien suunnittelussa tulisi siis ottaa huomioon skaalautuvuus. Lisäksi uusien toiminnollisuuksien lisäämisen hallintaan tarvitaan mekanismeja. Missiokriittisten järjestelmien kyberturvallisuuteen liittyy taas tasapainottelua läpinäkyvyyden, ulkoisen informaation hyödyntämisen, kontrollin ja organisaation käytänteiden kanssa. (Ciccozzi ym., 2017).

Missiokriittisille organisaatioille on tyypillistä hyödyntää viranomaiskäyttöön suunniteltuja digitaalisia radiostandardeja, kuten TETRA, TETRAPOL tai P25 (Fantacci ym., 2016), jotka kykenevät datan siirtoon. Näiden teknologioiden migraatio LTE-puolelle on nähtävissä, mutta LTE-standardi missiokriittiseen käyttöön on vasta tulossa (3GPP, 2017). Siispä varsinkin viranomaisorganisaatioille standardointiin liittyvä haaste on siirtyminen LTE-maailmaan.

Esineiden internetin tuottaman datan hyödyntäminen on haastavaa. Esineiden internet tuottaa tyypillisesti valtavia määriä heterogeenistä dataa, joka pitää käsitellä, säilöä ja analysoida (Lee ja Lee, 2015). Esineiden internetin käyttöönottoa harkittaessa onkin tärkeää määritellä ensin tavoiteltavat hyödyt, joiden pohjalta määritellään tekninen toteutus sekä suunnitelma datan hyödyntämiseksi operatiivisen toiminnan tehostamiseksi.

Kuten luvussa 2.2 argumentoitiin, että esineiden internetin hyödyt ovat riippuvaisia ennen kaikkea siitä, kuinka esineiden internetiä hyödynnetään operatiivisessa toiminnassa. Siispä myös missiokriittisen esineiden internetin ratkaisuja suunniteltaessa on haasteena ymmärtää tavoitteet, sekä mahdollisesti tarvittavat muutokset organisaatiotasolla prosesseissa ja rakenteissa.

Jotta esineiden internetin myötä tavoiteltavat hyödyt voitaisiin realisoida, syntyy organisaatiotasolla ainakin kaksi haastetta: miten organisaation toimintatapoja tai rakennetta tulee muuttaa, jotta esineiden internetistä saadaan toi-

vottu hyöty (Kranz, 2017), ja kuinka eri toimialojen rajat muuttuvat esineiden internetin myötä (Wortmann ja Flüchter, 2015). Organisaation tasolla byrokraattiset ja organisaatiokulttuuriin liittyvät haasteet hankaloittavat esineiden internetin laajempaa adoptiota (Fraga-Lamas ym., 2016).

TAULUKKO 1 Missiokriittisen esineiden internetin haasteita

| Haaste | Kuvaus | Lähteet |
|---|---|---|
| Standardointi | Yleisesti hyväksyttyjä standardeja on puutteellisesti. Esineiden internetille ei ole vielä yhtä yksiselitteistä määritelmää, ja lisäksi standardien tulisi voida soveltua missiokriittiseen toimintaympäristöön. Standardoinnilla voidaan varmistaa heterogeenisen laitteiston ja ohjelmiston yhteentoimivuus. | Fraga-Lamas ym., 2016, Atzori ym., 2010, Lee ja Lee, 2015 |
| Skaalautuvuus | Haaste liittyy siihen, kuinka hyvin järjestelmä kykenee pysymään suorituskykyisenä kovan rasituksen, ja esineiden tai datan määrän lisääntyessä. Skaalautuvuuteen kuuluu haaste korkeasta verkon rasituksesta, joka johtaa huoleen palvelun laadun ylläpidosta. | Fraga-Lamas ym., 2016, Al-Fuqaha ym., 2015, Atzori ym., 2010 |
| Yhteentoimivuus | Laitteiden ja ohjelmistojen suuri heterogeenisyys luo haasteita niiden saumattomalle yhteistyölle. Haasteeksi muodostuu reaaliaikaisten ja päästä-päähän ratkaisujen luonti. Mm. pilven hyödyntäminen ja toteutustapa vaativat tarkkuutta. Lisäksi verkkoteknologioiden yhteensovittaminen on oma haasteensa. | Fraga-Lamas ym., 2016, Lee ja Lee, 2015, Al-Fuqaha ym., 2015 |
| Hallinta | Valtava määrä heterogeenisiä laitteita luo haasteen vikojen, asetuksien, kirjanpidon, suorituskyvyn sekä kyberturvallisuuden hallinnalle. | Al-Fuqaha ym., 2015 |
| Turvallisuus ja luotettavuus | Laitteiston ja verkkojen tulee olla robusteja, ja niiden käytön turvallista. Palvelun tulee myös toimia ennakoidusti. | Fraga-Lamas ym., 2016, Al-Fuqaha ym., 2015 |
| Kyberturvallisuus | Haasteet liittyvät mm. tiedon salaukseen, yksityisyyteen sekä pääsynhallintaan. Kyberturvallisuusriskeihin liittyvät laitteiston ja verkon turvallisuus, väärinkäytökset, elektroninen sodankäynti sekä automaatio, joka ulottaa haasteet myös fyysiseen ulottuvuuteen. Esineiden internetin myötä lisääntynyt laitteiden määrä nostaa haasteita yksityisyy- | Lee ja Lee, 2015, Sadeghi ym., 2015 |

| | | |
|---|---|---|
| | den ja haavoittuvuuden suhteen. Nykyisten kyberturvallisuusratkaisujen haaste on, ettei niitä ole suunniteltu vastaamaan esineiden internetin mittakaavaa. | |
| Mobiliteetti ja saatavuus | Palveluiden odotetaan toimivan käyttäjän ollessa liikkeellä. Palvelut siis vaativat jatkuvuudenhallintaa sekä liikkuvuuden hallintaa (Engl. Mobility management). Lisäksi toteutuksen täytyy olla riittävän redundanssi. | Fraga-Lamas ym., 2016, Al-Fuqaha ym., 2015 |
| Datan käsittely, säilöntä ja analyysi | Datan halutusta laatutasosta tulee voida varmistua. Lisäksi data tulee voida säilöä luotettavasti, ja siihen tulisi olla pääsy lähes reaaliajassa. Datan hyödyntämiseksi ei toistaiseksi ole kehitetty johdonmukaista viitekehystä. | Lee ja Lee, 2015, Fraga-Lamas ym., 2016, Chen ym., 2012 |
| Organisaation rakenteen ja toimintatapojen muutos | Esineiden internet mahdollistaa uudentyyppisiä työskentelytapoja. Hyötyjen saavuttamiseksi on kiinnitettävä huomiota organisaation sisäisiin prosesseihin, ja joissain tapauksissa organisaation rakenteisiin. | Kranz, 2017, Fraga-Lamas ym., 2016 |
| Toimialojen rajojen muutos | Esineiden internet voi häivyttää organisaatioiden siiloutuneisuutta. Haaste syntyy, kun esineiden internet mahdollistaa yhden organisaation toimialan laajentumisen toiselle toimialalle. Missiokriittisillä organisaatioilla tämä voi tarkoittaa myös laajempaa yhteistyötä, josta syntyykin haaste, kuinka tämä yhteistyö organisoidaan. | Wortmann ja Flüchter, 2015 |
| Byrokratia | Haaste koskee erilaisia vaatimuksia määräystenmukaisuuteen ja byrokratiaan liittyen. | Fraga-Lamas ym., 2016 |
| Budjetti | Organisaatioiden loppukäyttäjät arvioivat budjetin suurimmaksi uusien sovellusten hankinnan esteeksi. | IHS Markit, 2017 |

# 4 YHTEENVETO

Tässä tutkielmassa pyrittiin ymmärtämään, mitä on missiokriittinen esineiden internet sen käyttöönottoa harkitsevan viranomaistahon näkökulmasta. Lisäksi esiteltiin näkökulmia, joita tulee ottaa huomioon siihen pohjautuvan ratkaisun hankintaa suunniteltaessa ja harkittaessa. Tutkielmasta on hyötyä käytännön tasolla, kun pyritään hankkimaan ymmärrystä siitä, mitä asioita ja näkökulmia missiokriittisestä esineiden internetistä tulee ottaa huomioon, jotta siitä voidaan hyötyä.

Tutkielman alussa käsiteltiin esineiden internetiä ICT- ja arvontuotannon näkökulmista. Esineiden internet tulee todennäköisesti mullistamaan sen, kuinka teemme työtä. Sillä on potentiaali rikkoa siiloja organisaatioiden sisällä, mutta se myös avaa uusia mahdollisuuksia yhteistyölle sekä organisaatioiden työnkuvan laajentumiseksi.

Esineiden internet rakentuu kolmen elementin ympärille. Nämä ovat esineet tai laitteet, yhdistettävyys sekä esineiden internet -pilvi. Esineet ja laitteet voidaan nähdä joko älykkäinä esineinä, aktuaattoreina tai käyttölaitteina, ja yhdessä esineessä tai laitteessa voi yhdistyä useampi näistä. Yhdistettävyyteen liittyy ne teknologiat, jotka mahdollistavat esineiden välisen vuorovaikutuksen ja tiedonsiirron pilveen. Pilvikerroksessa ratkaistaan esineiden internetin semantiikkaan liittyviä haasteita, eli kuinka dataa käytetään, esitetään ja tallennetaan.

Esineiden internetin hyötyjä tavoiteltaessa on myös olennaista ymmärtää, millaisia ongelmia tai haasteita esineiden internetillä pyritään ratkomaan. Tällä tarkoitetaan sitä, että hyötyjen tavoittamiseksi on ymmärrettävä, kuinka arvo muodostuu, ja että esineiden internetiä hyödynnettäessä on otettava huomioon tarvittavat muutokset operatiivisissa toimintatavoissa. Laajemmassa mittakaavassa esineiden internetiä tarkastellaan osana digitalisoituja palveluita. Luvussa 2.2 kuvattiinkin esineiden internet tässä kontekstissa.

Kolmannessa luvussa tarkasteltiin missiokriittistä esineiden internetiä erityisesti viranomaisten näkökulmasta. Järjestelmän katsotaan olevan missiokriittinen, kun sen vikautuminen voi johtaa merkittäviin vahinkoihin tai ihmishengen vaarantumiseen. Missiokriittinen esineiden internet perii pääpiirteittäin samat rakenteet, kuin esineiden internet. Missiokriittiselle esineiden internetille

on neljä erityistä ominaispiirrettä. Nämä ominaispiirteet ovat luotettavuus, turvallisuus, kyberturvallisuus ja reaaliaikaisuus. Vaikka tässä tutkielmassa painotettiin viranomaisnäkökulmaa, vaikuttaa kuitenkin siltä, että samat missiokriittiset ominaisuudet, mitä viranomaiskäyttö edellyttää, sopivat hyvin myös muihin missiokriittisiin käyttötapauksiin. Missiokriittisestä esineiden internetistä nostettiin esille myös muutamia haasteita.

Tutkielmalla on kaksi kontribuutiota. Tutkielman pääkontribuutio on missiokriittisen esineiden internetin teknologiapino (kuvio 2). Mallia voidaan hyödyntää missiokriittisen esineiden internetin ymmärtämiseen sekä sen toteutusten suunnittelun pohjana. Mallissa otetaan huomioon missiokriittiselle esineiden internetille tyypilliset neljä ominaisuutta: luotettavuus, turvallisuus, kyberturvallisuus sekä reaaliaikaisuus. Nämä ominaisuudet ovat määrittäviä tekijöitä nimenomaan missiokriittisissä järjestelmissä. Mallia voidaan käyttää pohjana missiokriittisen esineiden internetin ratkaisuille, sillä se kattaa olennaiset huomionarvoiset näkökulmat.

Missiokriittisen esineiden internetin teknologiapinon tueksi tutkielmassa esiteltiin esiinnousseita haasteita liittyen missiokriittiseen esineiden internetiin. Keskeisimmät haasteet vaikuttaisivat liittyvän teknologioiden määrään ja heterogeenisyyteen, järjestelmän skaalautuvuuteen ja turvallisuuteen, sekä prosessien muutokseen.

Toinen kontribuutio on, että pelkkä (missiokriittisen) esineiden internetin teknologiapino ei riitä kuvaamaan sitä, kuinka esineiden internetin myötä tavoiteltavat hyödyt voidaan saavuttaa. Hyötyjen saavuttamiseksi esineiden internetiä tulisi tarkastella palvelualustana, jonka ympärille muodostuu palveluekosysteemi, jossa arvonmuodostus tapahtuu toimijoiden välisenä arvon yhteiskehityksenä. Tässä kontekstissa missiokriittinen esineiden internet toimii mahdollistajana tavoiteltujen hyötyjen tuotannolle.

Tutkimusprosessin haasteeksi muodostui missiokriittisistä järjestelmistä tehdyn kirjallisuuden vähäinen määrä. Lisäksi missiokriittisistä järjestelmistä puhuttaessa aihetta käsiteltiin hyvin eri lähtökohdista. Jotkin artikkelit käsittelivät aihealuetta yritysten näkökulmasta, ja toiset taas väestönsuojelun ja katastrofiavun näkökulmasta. Jälkimmäinen liittyy tiiviimmin tämän tutkielman aihepiiriin. Tämän haasteen ratkomiseksi tutkielmassa käytettiin harkintaa, jotta tuotettu tietämys olisi mahdollisimman lähellä nimenomaan viranomaiskontekstia.

Jatkotutkimusaiheeksi ehdotan missiokriittisen esineiden internetin teknologiapinon sopivuuden tutkimista viranomaisten esineiden internetin ratkaisujen mallintamiseen. Myös missiokriittisen esineiden internetin arvonmuodostukseen tulisi perehtyä syvemmin.

## LÄHTEET

3GPP. (2017). Mission Critical Services in 3GPP. Haettu 16.4.2018, osoitteesta http://www.3gpp.org/news-events/3gpp-news/1875-mc_services

AIOTI. (2015). Working Groups. Haettu 15.4.2018, osoitteesta https://aioti.eu/working-groups/

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347-2376.

Agarwal, Y., & Dey, A. K. (2016). Toward Building a Safe, Secure, and Easy-to-Use Internet of Things Infrastructure. *IEEE Computer*, 49(4), 88-91.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, 54(15), 2787-2805.

Belanger, F., & Xu, H. (2015). The role of information systems research in shaping the future of information privacy. *Information Systems Journal*, 25(6), 573-578.

Beverungen, D., Müller, O., Matzner, M., Mendling, J., & vom Brocke, J. (2017). Conceptualizing smart service systems. *Electronic Markets*, 1-12.

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. *Proceedings of the first edition of the MCC workshop on Mobile cloud computing* (pp. 13-16). ACM.

Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business intelligence and analytics: from big data to big impact. *MIS quarterly*, 1165-1188.

Chen, C., & Helal, S. (2011). A device-centric approach to a safer internet of things. *Proceedings of the 2011 International Workshop on Networking and Object Memories for the Internet of Things* (pp. 1-6). ACM.

Chiang, M., & Zhang, T. (2016). Fog and IoT: An overview of research opportunities. *IEEE Internet of Things Journal*, 3(6), 854-864.

Ciccozzi, F., Crnkovic, I., Di Ruscio, D., Malavolta, I., Pelliccione, P., & Spalazzese, R. (2017). Model-Driven Engineering for Mission-Critical IoT Systems. *IEEE Software*, 34(1), 46-53.

Critical Communications World (2018). Haettu 13.4.2018, osoitteesta http://www.critical-communications-world.com/CCW

Fantacci, R., Gei, F., Marabissi, D., & Micciullo, L. (2016). Public safety networks evolution toward broadband: Sharing infrastructures and spectrum with commercial systems. *IEEE Communications Magazine*, 54(4), 24-30.

Fraga-Lamas, P., Fernández-Caramés, T. M., Suárez-Albela, M., Castedo, L., & González-López, M. (2016). A review on internet of things for defense and public safety. *Sensors*, 16(10), 1644.

Favraud, R., Apostolaras, A., Nikaein, N., & Korakis, T. (2016). Toward moving public safety networks. *IEEE Communications Magazine*, 54(3), 14-20.

Gartner (2018). IoT. Haettu 16.4.2018, osoitteesta https://view.ceros.com/gartner/iot/p/1

Gartner (2017): "Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent From 2016", haettu 11.11.2017 osoitteesta: http://www.gartner.com/newsroom/id/3598917

Giusto, D., Iera, A., Morabito, G., & Atzori, L. (2010). The internet of things: 20th Tyrrhenian workshop on digital communications. *Springer Science & Business Media*.

Girbal, S., Moretó, M., Grasset, A., Abella, J., Quiñones, E., Cazorla, F. J., & Yehia, S. (2013). On the convergence of mainstream and mission-critical markets. *Proceedings of the 50th Annual Design Automation Conference* (p. 185). ACM.

Grönroos, C., & Voima, P. (2013). Critical service logic: making sense of value creation and co-creation. *Journal of the academy of marketing science*, 41(2), 133-150.

Iansiti, M., & Lakhani, K. R. (2014). Digital Ubiquity: How Connections, Sensors, and Data Are Revolutionizing Business. *Harvard Business Review*, 92(11), 19.

IEEE (2014). Special Report: The Internet of Things. Haettu 15.4.2018, osoitteesta http://theinstitute.ieee.org/static/special-report-the-internet-of-things

IEEE Internet Initiative. (2015). Towards a definition of the Internet of Things (IoT). Revision-1, Haettu 15.4.2018, osoitteesta: http://iot. ieee. org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things _ Revision1_27MAY15. pdf.

Gonzales, J. (2017). Critical Communications LTE – End-user Survey Analysis. IHS Markit.

Knight, J. C. (2002). Safety critical systems: challenges and directions. *Proceedings of the 24rd International Conference on Software Engineering* (pp. 547-550). IEEE.

Kranz, M. (2017). Success with the Internet of Things Requires More Than Chasing the Cool Factor. Haettu 16.4.2018, osoitteesta https://hbr.org/2017/08/success-with-the-internet-of-things-requires-more-than-chasing-the-cool-factor

Lloret, J., Tomas, J., Canovas, A., & Parra, L. (2016). An integrated IoT architecture for smart metering. *IEEE Communications Magazine*, *54*(12), 50-57.

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, 58(4), 431-440.

Lusch, R. F., & Nambisan, S. (2015). Service innovation: A service-dominant logic perspective. *MIS quarterly*, 39(1).

Macedo, D., Guedes, L. A., & Silva, I. (2014). A dependability evaluation for Internet of Things incorporating redundancy aspects. *2014 IEEE 11th International Conference on Networking, Sensing and Control*, (pp. 417-422). IEEE.

Newell, S., & Marabelli, M. (2015). Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of 'datification'. *The Journal of Strategic Information Systems*, 24(1), 3-14.

OECD (2012), "Machine-to-Machine Communications: Connecting Billions of Devices", *OECD Digital Economy Papers*, No. 192, OECD Publishing.

Open Connectivity Foundation (2018). About Open Connectivity Foundation. Haettu 15.4.2018, osoitteesta https://openconnectivity.org/foundation

Pagani, M. (2013). Digital business strategy and value creation: Framing the dynamic cycle of control points. *MIS Quarterly*, 37(2).

Porter, M. E., & Heppelmann, J. E. (2014). How smart, connected products are transforming competition. *Harvard Business Review*, 92(11), 64-88.

Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial internet of things. *Proceedings of the 52nd annual design automation conference* (p. 54). ACM.

Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and challenges for realising the Internet of Things. *Cluster of European Research Projects on the Internet of Things, European Commision*, 3(3), 34-36.

Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the internet of things: a review. *2012 international conference on Computer Science and Electronics Engineering*, (Vol. 3, pp. 648-651). IEEE.

Tuunanen, T., & Cassab, H. (2011). Service process modularization: reuse versus variation in service extensions. *Journal of Service Research*, 14(3), 340-354.

Vargo, S. L., & Lusch, R. F. (2004). Evolving to a new dominant logic for marketing. *Journal of Marketing*, 68(1), 1-17.

Vargo, S. L., & Lusch, R. F. (2008). Service-dominant logic: continuing the evolution. *Journal of the Academy of marketing Science*, 36(1), 1-10.

Wortmann, F., & Flüchter, K. (2015). Internet of things. *Business & Information Systems Engineering*, 57(3), 221-224.